EXHIBIT 31

INTERNATIONAL STANDARD

ISO 22383

First edition
2020-09

Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for the selection and performance evaluation of authentication solutions for material goods

Reference number
ISO 22383:2020(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Principles ... **3**
4.1 General ... 3
4.2 Security-by-design process for authentication solutions ... 4
4.3 Categorization of authentication solutions ... 5
4.3.1 General ... 5
4.3.2 Provision of knowledge ... 6
4.3.3 Sourcing and production of authentication elements and tools ... 6
4.3.4 Inspection ... 6
4.3.5 Categories of authentication elements ... 7
5 Performance criteria specification based on risk analysis ... **8**
5.1 General ... 8
5.2 Risk analysis elements ... 9
5.3 Performance criteria categories ... 9
5.4 Criteria for selection of authentication elements ... 9
5.4.1 Physical characteristics ... 9
5.4.2 Attack resistance ... 10
5.4.3 Integration process ... 11
5.5 Attack-resistance criteria for selection of authentication tools ... 12
5.5.1 General ... 12
5.5.2 Obsolescence ... 12
5.5.3 Assessment of vulnerability and resistance of authentication tools ... 12
5.6 Criteria for selection of authentication elements and tools ... 12
5.7 Criteria for selection of authentication solutions ... 13
5.7.1 Location/environment for authentication process ... 13
5.7.2 Authentication parameters ... 13
5.7.3 Life cycle criteria ... 13
5.7.4 Security policy ... 13
5.7.5 Compliance with regulations, security practices and quality procedures ... 14
5.7.6 Operation ... 14
5.7.7 Ability to evaluate the performance of the authentication solution ... 14
6 Effectiveness assessment of authentication solutions ... **15**
6.1 General ... 15
6.2 Definition of effectiveness assessment protocols ... 15
6.3 Effectiveness assessment in manufacturing of authentication elements ... 17
6.4 Effectiveness of delivery of authentication elements ... 17
6.5 Effectiveness of application of authentication elements ... 17
6.6 Data management ... 17
6.7 Effectiveness measurement in normal verification/authentication situations ... 18
6.8 Effectiveness assessment in emergency verification/authentication situations ... 18
6.9 Impact of verification results and corrective actions ... 18
Annex A (informative) **Assessment grid** ... **19**
Annex B (informative) **Control means access table** ... **24**
Bibliography ... **25**

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 292, *Security and resilience*.

This second edition cancels and replaces the first edition (ISO 12931:2012), which has been technically revised. The main changes compared with the previous edition are as follows:

— it has a new ISO number and title, and is now included in the ISO 22300 family of standards;

— its terminology mirrors ISO 22300;

— relevant standards published since the first edition have been added as references.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Since the issuance of the first edition of this document in 2012, the quantity and range of material goods counterfeited or otherwise subject to product fraud continues to expand, and now affects many consumer goods and spare parts.

The sale of counterfeit goods, as well as falsified, illegally copied or illicitly traded products, is prevalent in many developing countries and is becoming more common in the developed world. Individual manufacturers and rights holders are experiencing an increase in the number of counterfeiting attacks on their material goods. The internet is compounding the problem. These counterfeit goods do not necessarily offer the same guarantees in terms of safety and compliance with environmental measures and regulatory requirements, generating risk for consumers, patients, users and the distribution chain. They cause loss of earnings, job losses and brand value damage for companies and targeted rights holders as well as tax losses for governments. Counterfeiting increases the potential for false material goods claims and litigation for companies and distribution supply chains. Counterfeiting of material goods has become one of the major activities of organized crime, both within domestic markets and international trade and smuggling.

In order to prevent counterfeiting and other types of product fraud, rights owners, institutions and governmental regulators are increasingly demanding and implementing authentication solutions geared to specific needs. It is important to specify the performance requirements for the solutions designed to support the fight against counterfeiting at both national and international levels. This will promote greater confidence among consumers, support the security of the supply chain, and help public authorities devise and implement preventive, deterrent and law enforcement policies. In addition, the growth of global trade and the reduction of physical controls at borders has increased the risk of more counterfeited products in circulation. This document will contribute to further strengthen such controls by enabling faster and more reliable evidence of the authenticity and integrity of material goods.

Product fraud includes, but is not limited to, counterfeiting, adulteration, tampering, substitution and simulation.

Product fraud impact can include, but is not limited to:

— deception of the consumer;

— deception of the purchaser of new goods or replacement parts;

— infringement of intellectual property rights;

— violation of national, regional or international laws;

— false claims regarding:

  — intellectual property rights;

  — details of manufacture;

  — trade and origin details;

  — identification codes and/or authentication elements.

The problem of product fraud is aggravated by the following factors:

— the market is increasingly global;

— the material goods and their supply chains are more complex;

— the global movement of material goods is increasing and can use non-traditional channels.

Counterfeiting needs to be kept separate from diversion.

It can be difficult for an inspector, be it a dedicated professional or any citizen or consumer, to recognize the characteristics of a given authentic material good.

Counterfeiting seeks to bypass legal provisions, including guarantees of conformity and quality, designed to enable professionals to release safe material goods into the market in fair competition. Buyers do not necessarily pay all the attention needed to the material goods they are examining, particularly due to trust, lack of time, the temptation of attractive prices or simply because they are unfamiliar with the material good itself. The authentication element provides a specific and more reliable method of determining whether the item is genuine or a counterfeit good.

Establishing the authenticity and integrity of a material good, in other words recognizing whether it is genuine or fake or otherwise subject to fraudulent activities, requires checking whether it reproduces the essential characteristics of the authentic material good, to help establish whether or not there has been an infringement.

If there is any doubt as to the authenticity of a material good, it is the inspectors' role, once they have observed the characteristics of the suspect material good and/or authentication element, to verify whether these characteristics match those of the authentic material good and/or authentication element. The process involved is an essentially technical analysis using experience, authentication elements, authentication tools or a combination of these methods.

This document has been drafted to pinpoint the objectives and boundaries required for industry-wide and services-wide application. It sets out the performance criteria for purpose-built authentication solutions.

These solutions are designed to provide reliable evidence, making it easier to assess whether material goods are authentic and have not been counterfeited, altered, mimicked, replaced, refilled, tampered or subject to other types of product fraud.

This document integrates the performance requirements for authentication solutions. The material good's life cycle needs to be considered. Whereas authentication of fast-moving consumer goods often concentrates on packaging, authentication solutions of material goods with longer life cycles instead aim at the material good itself, throughout its life cycle.

This document is part of a wider framework of related standards. It was not drafted or designed to define any exclusive means of authentication.

Experience shows that advancements in technologies are exploited by counterfeiters to make counterfeited products less detectable. At the same time, new authentication technologies (e.g. material, digital and combined) can give law enforcement inspectors, legitimate economic operators and consumers better means to detect counterfeits and act accordingly. This document is applicable irrespective of the authentication technology used and recommends ways to stay ahead of fraudsters.

This document therefore includes:

— a common categorization of authentication solutions;

— an understanding of how an authentication solution can constitute a more robust solution when layered, and therefore it promotes the use of individual authentication elements in combination;

— the role of tamper resistance and tamper evidence as part of an authentication solution;

— criteria for the types of solution that can be used to authenticate in different verification scenarios;

— methods to enable material good verifications in all intended locations, circumstances and conditions of use;

— requirements and evaluation criteria on security for the authentication solutions.

The main topics of this document can be represented as a Plan-Do-Check-Act (PDCA) cycle, see Figure 1.

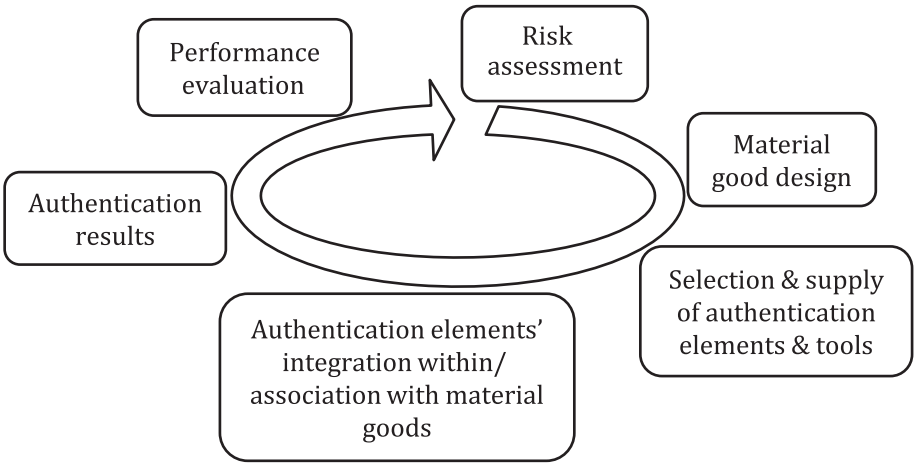

Figure 1 — Sequence of the main topics

Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for the selection and performance evaluation of authentication solutions for material goods

1 Scope

This document gives guidelines for performance criteria and an evaluation methodology for authentication solutions that aim to unambiguously establish material good authenticity and integrity throughout an entire material good's life cycle. It focuses on the authentication of a material good and, if appropriate, its components, parts and related data:

— covered by intellectual property rights;

— covered by relevant international, regional or national regulations;

— with counterfeiting-related implications;

— otherwise with a distinctive identity.

This document is applicable to all types and sizes of organizations that require the ability to validate the authenticity and integrity of material goods. It will help organizations to determine the categories of authentication elements they need in order to combat counterfeiting-related risks, and the criteria for selecting authentication elements, after having undertaken a counterfeiting risk assessment.

Authentication solutions can be used in areas such as anti-counterfeiting, prevention of product fraud and prevention of diversion.

This document does not specify economic criteria aiming to correlate performance and costs of the authentication solutions.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies:

ISO 22300, *Security and resilience — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
attack
successful or unsuccessful attempt(s) to circumvent an authentication solution, including attempts to imitate, produce or reproduce the authentication elements

3.2
covert authentication element
authentication element that is hidden from the human senses until the use of a tool by an informed person reveals it to their senses or else allows an automated interpretation of the element

[SOURCE: ISO 22300:2018, 3.58, modified — The definition has been rephrased.]

3.3
integrity
property of safeguarding the accuracy and completeness of assets

Note 1 to entry: Assets relate to material goods and its primary packaging.

Note 2 to entry: Integrity also concerns the associated data, information or the elements and means for their processing.

[SOURCE: ISO 22300:2018, 3.123, modified — Notes 1 and 2 to entry have been added.]

3.4
raw material
any element, constituent or part of a material good

3.5
rights holder
physical person or legal entity either holding or authorized to use one or more intellectual property rights

[SOURCE: ISO 22300:2018, 3.198, modified — "physical person or" has been added.]

3.6
security
state of being free from danger or threats where procedures are followed or after taking appropriate measures

[SOURCE: ISO 22300:2018, 3.223, modified — "where procedures are followed or after taking appropriate measures" has been added.]

3.7
simulation
imitative representation of the functioning of one system or process by means of the functioning of another

3.8
specifier
person or entity who defines the requirements for an authentication solution to be applied to a particular material good

[SOURCE: ISO 22300:2018, 3.246, modified — "person or" has been added.]

3.9
tamper evidence
ability of the authentication solution or the authentication element to show that the material good has been compromised

[SOURCE: ISO 22300:2018, 3.254, modified — "the authentication solution or" has been added.]

3.10
track and trace
means of identifying every individual material good or lot(s) or batch in order to know where it is at a given time (track) and where it has been (trace) in the supply chain

[SOURCE: ISO 22300:2018, 3.264, modified — "where it is at a given time (track) and where it has been (trace)" has replaced "where it has been (track) and where it is (trace)".]

3.11
verification
confirmation, through the provision of evidence, that specified requirements have been fulfilled

Note 1 to entry: Verification can include checking that a unique identifier exists and is valid within an object identification system.

4 Principles

4.1 General

The organization should select the most appropriate authentication elements to form an authentication solution for a material good, based on a risk assessment and on the context of implementation and usage.

When selecting an authentication solution, the organization should consider the technical, logistical and financial criteria, which will depend on numerous factors including:

— the characteristics of the authentication element(s);

— verification methods;

— any required information system;

— security requirements;

— counterfeit resistance;

— resilience against tampering;

— value of the material goods intended to be protected;

— counterfeiting risks throughout the material good's life cycle;

— integration and implementation requirements;

— the role of packaging;

— evidence of forged, counterfeited or copied features.

The organization should not select an authentication solution that affects or alters, in an uncontrolled way, the intended functionality and the integrity of the material goods.

NOTE Authentication elements can be part of the functionality of a product, for example, in the security-by-design approach whereby the security is embedded at the stage of product conception.

The organization should be aware of applicable laws and regulations especially on privacy and safety.

In order to establish an authentication solution for a material good, a creation process must be followed by an inspection process. The creation process consists of defining, generating and manufacturing the authentication elements and integrating them with the material good or its packaging. The inspection process includes verifying the authentication elements along the distribution chain by trained people using human senses, tools or references. Those two processes are linked in the PDCA cycle and the actors involved form an integral part of the authentication solution.

The verification processes of authentication elements deployed in these solutions require the ability to read, capture and sometimes perform sampling using human senses or tools. These tools will either offer a local on-the-spot response or will call, in real-time, into a secure information system, or possibly re-channel the data, sample or material good towards a structure offering expert analysis for an off-line diagnosis.

The level of performance of an authentication solution should therefore be assessed as a whole, including all the components and interfaces involved.

As a strategy analysis, the main questions to be addressed by the rights owners are as follows.

— What are the counterfeiting issues and threats?

— What is the likelihood and what are the consequences of the counterfeiting risks on my products, organization and business?

— Which of my material goods (or its raw materials) are being counterfeited or have the potential to be counterfeited?

— In which locations are we experiencing counterfeiting and how are the counterfeits being distributed?

— What is the material good manufacturing and supply chain environment and risks of counterfeiting?

— What is the raw materials' manufacturing and supply chain environment and risks of counterfeiting?

— How and by whom will the authentication process be performed?

— What is the impact of human error on the solution (process and authentication)?

4.2 Security-by-design process for authentication solutions

The organization should follow the process diagram given in Figure 2 when designing its authentication solution. This process includes a proper analysis of the risks associated with the characteristics of a material good, including its raw materials, the options for its authentication, and the consequences and history of counterfeiting acts such as adulteration, tampering, substitution/refill, simulation, cloning or diversion.

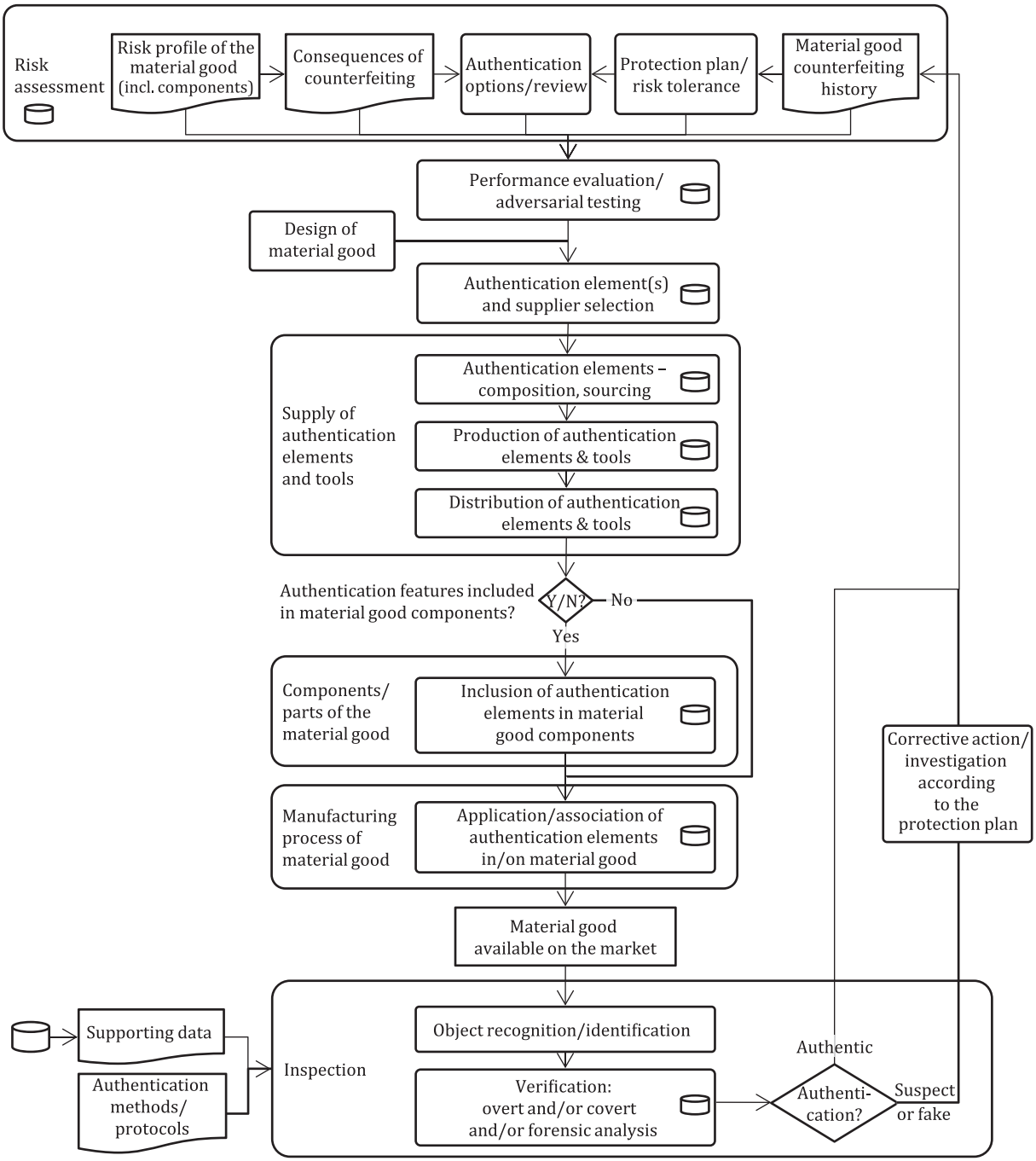

Figure 2 — Functional block diagram of a typical authentication solution

4.3 Categorization of authentication solutions

4.3.1 General

This categorization is intended to provide a guideline for users and suppliers of authentication solutions that allow the solutions to be compared or selected according to their characteristics. It is not intended to rank the solutions according to performance effectiveness. The environment of the examination helps to determine the choice of the authentication solution(s).

The characteristics used in this categorization are based on the considerations given in 4.3.2 to 4.3.5.

4.3.2 Provision of knowledge

4.3.2.1 General

Any authentication solution will require some knowledge to be provided to the inspector. An inspector uses the authentication solution with the aim of authenticating a material good.

Without the knowledge that a certain authentication solution has been applied to the material good in question, an inspector cannot inspect the associated authentication element. Without knowledge of the appropriate inspection procedure, the inspector cannot adequately perform the authentication. The knowledge required can be subdivided into general knowledge (e.g. how a class of authentication elements appears to the inspector) and material good-specific knowledge (e.g. which particular authentication element has been applied to the material good being inspected). However, the rights holder can control the target audience of this knowledge, in particular for material good-specific knowledge. The distinctions given in 4.3.2.2 and 4.3.2.3 are used for the categorization.

4.3.2.2 General audience

Knowledge about the authentication solution employed is made public, for example, via advertisements, websites or marketing materials.

4.3.2.3 Restricted audience

Knowledge about the authentication solution employed is made available only to a restricted group of people that have a need to know. This will usually include all those people who are professionally required to inspect the material good, and thus excludes those in the general audience. This approach is limited by the potential risk that the knowledge will leak from the intended audience and could ultimately become public knowledge. On the other hand, the security of an authentication solution can be substantially increased by restricting the availability of knowledge.

4.3.3 Sourcing and production of authentication elements and tools

The providers of both authentication elements and tools should be registered and subject to an independent audit of their capabilities, procedures, records and evidence of security measures.

The design, production and distribution of authentication elements should be protected against knowledge transfer. The production of the authentication tools should also be securely protected against theft or other illicit activities.

4.3.4 Inspection

4.3.4.1 General

The process of inspection of an authentication element invariably involves some form of physical observation. The three types of inspection method are given in 4.3.4.2 to 4.3.4.4.

A legal authority can often require that evidence of inspection results be established by a trusted third party through forensic analysis.

4.3.4.2 Human senses

The inspector uses his or her eyes, ears, hands, nose, etc. to inspect the material good.

4.3.4.3 Authentication tool

An authentication tool is employed to perform the required inspection and to display the result in some appropriate way for presentation to the inspector. The tool employed may either be a field-available tool or require the use of a laboratory equipment or similar environment.

The organization should consider the categorizations described in Table 1 when comparing and selecting authentication solutions. There are two types of audience when it comes to the knowledge of the inspection procedure needed to adequately perform the authentication: the general audience (see 4.3.2.2) and the restricted audience (see 4.3.2.3).

If the solution is designed for digital verification, it can lead to the detection of counterfeit by algorithms, which could be assessed by an inspector.

NOTE 1 In such a case, the presence of the information in the form of encrypted data, electronic signatures, visible digital seals[9] and comparable technologies can provide useful help in conducting the identification and/or authentication by any category of inspector.

NOTE 2 Identifiers of individual products, track and trace, or monitoring the supply chain are widely used. However, when used alone, track and trace technologies cannot be considered to be authentication solutions.

NOTE 3 Track and trace technologies can utilize databases, distributed ledgers such as blockchains, or others. They can be combined with authentication solutions if the assessment/control/inspection is expected to cover both aspects.

When an authentication solution uses an authentication tool to inspect the authentication element, this tool can be characterized by the following alternatives:

a) stand-alone or online (connected to a network permanently, or during time slots or in batches, to be able to interpret the authentication element);

b) purpose-built or commercial off-the-shelf.

Annex B provides a tool to define an anti-counterfeiting strategy in relation to the inspection of authentication elements.

4.3.4.4 Forensic analysis

The inspector will require dedicated scientific methods to perform the inspection. While forensic analysis may be performed in the field for authentication, it is more commonly performed in a laboratory setting with the use of common and specialized scientific equipment and processes for examination.

4.3.5 Categories of authentication elements

4.3.5.1 General

The validation process for all the categories of authentication elements categories often uses original exemplars for a comparative analysis. The characteristics of categories are given in Table 1 and are explained in 4.3.5.2 to 4.3.5.4.

Table 1 — Characteristics of categories for tailored authentication solutions

	Human senses	Authentication tool		Forensic analysis
		Off-the-shelf[a]	Purpose-built	
General audience	OVERT	COVERT	—	—
Restricted audience	OVERT	COVERT	COVERT	COVERT
[a] This can include smart consumer devices (e.g. smartphones, tablets).				

4.3.5.2 Overt category

Overt authentication can be directly performed by an informed inspector and does not require any additional equipment to allow a feature to be verified as genuine.

Overt authentication elements are apparent to the human senses, most often sight but touch is also used. Overt authentication elements are often therefore employed where a visual check is the only one

immediately possible and this can be undertaken by informed inspectors, such as consumers, store clerks and check-out staff.

Ideally the inspector will have a genuine authentication element as a reference comparison.

Overt authentication elements must be difficult to copy accurately so that their absence or their imperfections will alert examiners to the fact that a material good may not be genuine, because counterfeiters will always try to reproduce all visible features on the material good and its packaging in their effort to produce a realistic copy. The absence of an overt authentication element or the presence of a crude copy, therefore, is an indication that the material good is probably not genuine.

4.3.5.3 Covert category

Covert authentication elements are not instantly recognizable or interpretable by human senses. They require authentication tools and/or specialized knowledge to verify their presence and validity, either revealing themselves to the human senses (usually vision) or to the authentication tool. These tools can be stand-alone or require a connection to a network and be off-the-shelf or purpose-built. The result presented by an authentication tool could determine the authentication element's authenticity or the decision could be left to the inspector. Inspectors analysing these authentication elements need some training.

Covert technologies exploit all kinds of physical, chemical or biological effects, as well as logical relationships. Electronically supported authentication elements use software- or/and hardware-based data and/or protocols securely related to the genuine material good for proof of authenticity.

Covert authentication solutions may be designed so that authentication can be performed in the field.

Where covert authentication solutions use data that are or can be linked to a person, privacy principles and regulations should be identified and taken into account.

With the evolution of technology, a general audience will have the capacity to authenticate a covert authentication element, subject to specific conditions as determined by the authentication solution specifier.

4.3.5.4 Forensic category

Forensic authentication elements require the use and knowledge of dedicated methods and tools to evaluate the authentication elements or intrinsic attributes of a material good (e.g. forensic taggants, fingerprints). Forensic authentication elements are generally detected or checked in a specialized laboratory.

5 Performance criteria specification based on risk analysis

5.1 General

The organization should consider the following performance criteria when comparing and selecting authentication solutions. These performance criteria will make it easier to determine that the authentication solutions meet the needs and requirements of the user. This includes:

— criteria for the selection of authentication elements (see 5.4);

— criteria for the selection of authentication tools (see 5.5);

— criteria for the selection of authentication solutions (see 5.7).

NOTE Annex A provides a grid by which the specifier can select the criteria.

5.2 Risk analysis elements

The organization should identify the key risk aspects for the optimal selection of the authentication elements and tools, such as:

— risk profile of the material goods;

— consequences of counterfeiting;

— authentication options;

— suppliers (and history) of authentication elements;

— counterfeiting history of the material goods.

5.3 Performance criteria categories

Based on specific risk assessment, including the fraud history and authentication options, the organization may select an authentication solution that combines several authentication elements working together to build proof. These elements may be of different types (overt, covert and forensic) and with different levels of accessibility. Several performance criteria of authentication solutions may be considered for the following different categories (stated in alphabetical order):

— ability to provide information feedback or analytical results;

— attack resistance;

— field/environmental function;

— implementation process;

— integration process;

— physical characteristics;

— user friendliness.

A specifier may also choose to adopt an authentication solution that combines several authentication elements working together to build proof. These elements may be of different types (overt, covert and forensic) and with different levels of accessibility.

NOTE 1 A more robust authentication solution for a more reliable result can require more advanced expertise of the inspector.

NOTE 2 Annex A provides assessment criteria, parameters and criticality.

NOTE 3 For risk assessment, see ISO 31000.

NOTE 4 For product fraud, see ISO 22380.

5.4 Criteria for selection of authentication elements

5.4.1 Physical characteristics

The organization should consider the following physical characteristics when deciding what are the authentication elements to use.

— Static characteristics, such as size, thickness and weight. These characteristics have to be considered according to the material good, including the available space, compatibility and potential interference with material good features or process (see the integration process characteristics in 5.4.3).

— Dynamic characteristics, such as flexibility, viscosity, tear and tensile strength. If process requirements alter or damage the authentication elements, they will become unusable and cause the material good to be rejected during the final production control. Therefore, the organization should choose the authentication element considering any of the process requirements involved in the production of the material good.

— Durability characteristics, such as mild environmental conditions (climate features such as temperature and humidity), harsh environmental conditions (degradation features such as chemical action and radiation), mechanical use typical of the material good under consideration, and aging that can result in a malfunction of the authentication element over the life cycle of the material good.

  The organization should choose the authentication element considering these environmental conditions during processing, storage or operation that will not affect the physical characteristics of the authentication element in an adverse manner.

  The specifier of the authentication solution should define the conditions of usage based upon the required risk analysis. In addition, the life cycle of the material good can have a significant impact in determining the durability of the authentication capability.

— Health and environmental impact characteristics, such as electromagnetic radiation, radioactivity, chemical composition and banning of some substances, migration of substances and recyclability. The potential environmental and health impacts of authentication elements should be considered, particularly in light of national, regional and international regulations.

— Feature-linked physical characteristics, such as visibility, machine readability, tamper evidence and uniqueness (one-to-one, one-to-many). A feature can be recognized as unique in two manners, one-to-one or one-to-many. A unique feature that authenticates a single item and is unique only to that item is recognized as one–to-one. A unique feature applied to several items is recognized as one-to-many.

5.4.2 Attack resistance

The organization should select authentication elements that are able to withstand attacks. The authentication element should be resistant to the following.

— Reverse engineering: It should be extremely unlikely to acquire enough information to be able to successfully create/generate/manufacture an authentication element and to use this element to circumvent the material good protection. It should require an extraordinary level of effort to accurately copy authentication elements. If an authentication element were to be copied, the authentication element should contain copy-evident features apparent in the authentication process.

— Tampering: A tangible or intangible form of interdependence between the authentication element and the material good it protects should be developed. An authentication element displays tangible interdependence if it is destroyed or displays some form of visible or recognizable alteration when an attempt is made to remove the authentication element from the material good. Intangible interdependence occurs where the authentication element has a logical link to the material good or a reference that cannot be erased or duplicated. To generate tamper evidence, the various forms of interdependence should be affected by any (at least partly) serious attack, which is why an attack should immediately and irreversibly change one or more characteristics of the association between the authentication element and the material good, including its packaging. Furthermore, any changes to these characteristics resulting from an attempted attack should be detectable during the verification protocol. To reduce the chance of a false positive, the interdependent characteristics should remain stable and resist changes in environmental conditions during the material good's life cycle.

— Alteration: The authentication element should withstand modification of its characteristics or the modification of the information contained within the element. In the event the element is circumvented, detection of the attempt should be evident to the inspector.

— Side channelling: It should not be possible to capture any secret information or determine characteristics of the authentication element through analysis of its physical behaviour in any environmental circumstances.

— Security of data: The organization should ensure that data related to the production and its authentication elements are protected against attacks.

— Interception of communication: It should not be possible to gain attack-sensitive information by intercepting the communication between the authentication element and any tool required to read or verify the element. Thus, the authentication element either should not communicate any attack-sensitive information with the tool or the information exchange should be secured.

— Obsolescence: The organization should evaluate the potential longevity of the authentication element, the degree the element will remain an effective solution, and the availability of the technology and support in the future.

— Non-controlled reuse: The organization should ensure that the authentication element cannot be re-used without authorization.

— Data: The organization should ensure that data related to the production and the data authentication elements are protected against attacks.

5.4.3 Integration process

5.4.3.1 General

The organization should ensure that the integration process of the authentication elements with the material good and/or its packaging is performed under secure conditions.

5.4.3.2 Manufacturing

— Availability: The organization should ensure that the integrator can meet the production and supply requirements for the authentication element and its integration into the material good or its packaging.

— Compatibility: The authentication element should be compatible with the material good or its packaging, the process and logistics. The impact of the authentication element on the manufacturing and distribution processes should be evaluated.

  In the selection of authentication technologies, the necessity for simultaneous reading and aggregation requirements and potential collisions should be taken into consideration.

— Integrity: The organization should secure the machines involved in manufacturing so that non-authorized alterations of systems and processes are detected.

  The organization should report any attempt to hack or tamper these machines to the appropriate authorities.

5.4.3.3 Compliance

Depending on the business case and the regulatory requirements, the organization should conduct independent audits, ensuring that all of the integration requirements are being met and can be verified.

5.4.3.4 Training

The organization should consider the appropriate level of training for each involved party, depending on their authority, in all phases of the integration process in order to support the best performance of the authentication solution.

5.5 Attack-resistance criteria for selection of authentication tools

5.5.1 General

Depending on the requirements, the organization should select authentication tools that are:

— resistant to attacks that can be used to recover secret or sensitive information, which could lead to the ability to create/generate/manufacture an authentication element;

— resistant to the creation of a fake authentication tool that could be considered by an inspector to be legitimate;

— protected and/or react to any physical attempt of deviation aimed to capture information that is processed or transferred;

— protected against attempts to capture any confidential data or characteristics of the authentication tool through analysis of its physical behaviour or interaction with the authentication element in any environmental circumstances;

— protected against any unauthorized communication between the authentication element and the tool and between the tool and the remote components of the authentication solution;

— protected against any intrusion to reference databases;

— protected by an authentication of the inspector (or both inspector and tool) to access any database used for the authentication process;

— capable of detecting and reporting tampering attempts to appropriate authorities;

— supported by a back-up system (data and redundancy service) to avoid interruption of service;

— resistant to the creation of a fake authentication website and/or services that could be considered by an inspector to be legitimate;

— protected against any intrusion to reference databases and other related data, e.g. with data integrity systems.

5.5.2 Obsolescence

The obsolescence of authentication elements and tools should be taken into consideration and managed.

5.5.3 Assessment of vulnerability and resistance of authentication tools

The organization should determine the attack resistance of an authentication solution by assessing its vulnerability and resistance to the types of attacks (threats) identified above and based upon a risk analysis of the material good (see ISO 31000, ISO/IEC 15408-1 and ISO/IEC 27002).

5.6 Criteria for selection of authentication elements and tools

The organization should consider the following criteria when selecting the supplier of the authentication elements and tools:

— undergo an independent audit of the supplier’s capabilities, procedures, records and evidence of security measures;

— verify that authentication elements originate from components that are not easily available on the market;

— verify that the production of authentication elements is protected against knowledge transfer about their composition and/or manufacturing process;

— verify that production of the authentication tools is securely protected against malicious acts;

— verify that data protection and integrity mechanisms are in place, regardless of the type of authentication tool selected to verify such data.

5.7 Criteria for selection of authentication solutions

5.7.1 Location/environment for authentication process

The organization should consider the following criteria for selecting the operating conditions for where the authentication process is performed. The locations of the authentication process should:

— provide required resources, such as power, communications and facilities;

— meet appropriate ambient environmental conditions, such as temperature, humidity, air pressure, electrostatic and magnetic fields, electromagnetic radiation and cleanliness, and external weather conditions;

— not be subject to exposure to hazardous conditions, such as a chemical, radioactive or explosive atmosphere;

— not cause deterioration during normal usage;

— support required ergonomic conditions, especially if the inspector needs to use human senses;

— have lighting conditions appropriate to read authentication elements or read results if the control is done using a tool.

5.7.2 Authentication parameters

The organization should consider the following criteria for the selecting the operating conditions for how the authentication process is performed. The following parameters should be stated for the authentication process:

— the necessary time to process an authentication;

— the number of successive accurate authentications per unit of time;

— the dependency of the response time on the number of concurrent authentications;

— the necessary time to get an authentication result.

5.7.3 Life cycle criteria

The life cycle of tools should be managed so that the introduction of new tools in an authentication solution is possible while maintaining the level of security of the solution.

Supporting equipment (e.g. IT systems and infrastructure) should be managed so that backward compatibility and level of security are guaranteed for a period of time to be specified by the rights holder.

This concerns either the information related to authentication elements stored in data repositories or any equipment used to make the authentication solution work.

5.7.4 Security policy

The organization should establish a security policy for authentication solutions. The security policy should:

— concern all the components of the solution;

— include the security of the supply chain of the authentication solutions and any involved information technologies;

— be in accordance with relevant standards and resolutions, or recognized industry practices.

5.7.5 Compliance with regulations, security practices and quality procedures

The organization should identify and take into account all regulations from governmental or regulatory agencies applicable to the authentication solution. Special consideration should be made if the solution is to be implemented in international markets or used in international trade where regulations vary by country or region. Solutions used by governmental agencies can also be subject to specific regulations, procedures or requirements and privacy regulations that have to be taken in account.

The organization should ensure that the authentication solution is audited for compliance with security assurance and quality procedures. The audits should be performed according to relevant international or national standards, or recognized industry practices, by approved auditors or other authorities.

5.7.6 Operation

The organization should ensure that the authentication solution:

— is adapted to accommodate an increased volume of authentications;

— is upgradable without compromising its effectiveness;

— has quality and quantity of authentication elements and tools according to the solution specifications;

— includes the necessary training plan for each level of inspection;

— considers its potential impact on human health and the environment;

— can be inspected by an inspector with appropriate knowledge.

The organization should ensure that the authentication tool:

— fulfils requirements for a cold start or wake-up delay;

— does not interfere with the verification of another material good when used to verify different material goods at the same time;

— has acceptable rates of false acceptance and false rejection defined by the specifier, and such rates remain within the limits of variation of the environmental operational conditions defined by the manufacturer;

NOTE Methods to assist the calculation of acceptable rates include, but are not limited to: cumulative match characteristics (CMC), true positive identification rate (TPIR), area under receiver operating characteristic curve (ROC curve) known as AUR[10].

— can acceptably operate with reduced functionality either with its own power source or in online mode;

— is adequately supplied and maintained to meet the expected performance

5.7.7 Ability to evaluate the performance of the authentication solution

The organization should select an authentication solution that includes or supports the collection of data by the authentication tool and/or inspector, and reports results with regards to its efficiency and performance. Such reports may be produced in real time, in deferred time or on a periodic basis.

6 Effectiveness assessment of authentication solutions

6.1 General

The organization should perform an effectiveness assessment of the authentication solution to evaluate if it conforms to the established criteria and provides expected results.

The organization should define an assessment strategy in relation to the consideration of the material good's authenticity, integrity and product fraud issues (as described in ISO 22380). A material good can face a risk situation based upon the following categories.

a) The material good is not yet on the market: Prior to the introduction of a material good to the market, a risk analysis should be performed to determine likelihood of fraud, and if there are financial, legal, social, health, safety or regulatory issues that require the implementation of an authentication solution.

b) The material good is already on the market and no product fraud has been detected. This can be the result of multiple factors, such as:

   1) the authentication solution is effective:

      i) the material good and/or the authentication elements are very difficult to counterfeit;

   2) the authentication solution is not effective:

      i) the implemented authentication solution is ineffective, badly implemented or incorrectly inspected; in this case, fraud could exist and remain undetected;

      ii) adequate research or reporting has not been done to determine if the material good is counterfeited;

   3) the authentication solution is not present:

      i) there is little or no value in counterfeiting or protecting the material good.

c) The material good is already on the market and product fraud has been detected: In this condition, a material good is being counterfeited and the scale of counterfeiting is either known or unknown to the material good supplier. If the level of counterfeiting is known, then an effectiveness assessment can be established based upon a reduction in the number of known counterfeits, provided the reduction can be effectively traced to the authentication solution. If the level of counterfeiting is unknown, then an estimate of this number needs to be established by research and/or statistical analysis. Based upon the analysis, an estimation can be made of the effectiveness of the solution. Grey market issue is out of scope of this document.

The organization should conduct a risk assessment to determine the threat of counterfeiting, and if there are financial, legal, social, health, safety or regulatory issues that should be considered to determine if an authentication solution is necessary for the material good.

When the material good is already on the market, the variation of the sales curve can reflect an evolution of the counterfeiting situation. However, the response to counterfeiting issues needs more indicators to be efficient, including adding that external (non-technical) actions could have caused the variation.

6.2 Definition of effectiveness assessment protocols

Defining a standard that would encompass all of the unique effectiveness assessment protocols in addition to the authentication protocols is not feasible. The following key points should be considered by solution specifiers.

An effectiveness assessment is the evaluation of the selected solution to meet the requirements of the selection criteria, that is, how well the selected solution meets each of the following categories of criteria:

— physical characteristics;

— attack resistance;

— integration process;

— field / environmental function;

— implementation process;

— user friendliness;

— ability to provide information feedback or analytical results.

The assessment of effectiveness can be done by answering the questions associated with the following criteria:

a) Evaluation of the physical characteristics: Does the solution meet each of the specified physical characteristics: dimension, tensile strength, dimensional stability, flexibility, etc.? Are these characteristics measurable and definable in a specification? Can they be maintained consistently to meet quality assurance levels?

b) Evaluation of the attack resistance: Does the solution meet the specified attack resistance criteria: copying, hacking, tampering, etc.? Are these characteristics measurable and definable by specification? Can they be maintained consistently to meet quality assurance levels?

c) Evaluation of the integration process: Based on all the physical characteristics, is the integration process capable of a successful integration of the solution? Are these characteristics measurable and definable by specification? Can they be maintained consistently to meet quality assurance levels?

d) Evaluation of the field/environmental function: Does the solution meet the field/environmental function criteria: environmental conditions, hazardous conditions, etc.? Are these characteristics measurable and definable by specification? Can they be maintained consistently to meet quality assurance levels?

e) Evaluation of the implementation process: Based on all the characteristics, is the implementation process capable of a successful implementation of the solution? Are these characteristics measurable and definable by specification? Can they be maintained consistently to maintain the level of authentication required by the specifier?

f) Evaluation of user friendliness in terms of information and usage: An authentication solution can address one or several categories of users. These may include, but are not limited to:

   1) investigators authorized and trained by the rights holder;

   2) customs authorities;

   3) supply chain participants;

   4) professional users;

   5) consumers.

g) Ability to provide information feedback or analytical results: Is the solution able to provide feedback to the rights holder on the product fraud situation in the market, and to what degree?

The effectiveness assessment of the solution can be determined based upon an overall evaluation of the criteria selection process, the counterfeit environment of the material good, and the expectations of the risk analysis.

6.3 Effectiveness assessment in manufacturing of authentication elements

The organization should ensure that the manufacturing of the authentication solution conforms to quality requirements and should assess the effectiveness in manufacturing by the following evaluations:

— the number of false rejections in the final control of production, meaning that the authentication elements are out of tolerance or an anomaly in the process makes the authentication element unreadable;

— the number of false rejections on site, meaning that the authentication element's characteristics or association with the material goods are not stable;

— the number of false acceptances; this evaluation requires a specific control protocol, which should include an attempt to produce false authentication elements that pass the authentication control with success. Typically, this protocol is implemented by independent laboratory.

Security aspects should be managed, measured and recorded in accordance with relevant applicable standards (e.g. ISO 14298 for security printing).

6.4 Effectiveness of delivery of authentication elements

The chain of custody should be managed by the organization's customer-supplier relationship to ensure the appropriate security of the supply chain.

6.5 Effectiveness of application of authentication elements

The organization should:

— assess the process of affixing or integrating the authentication element to the physical item considering aspects such as surface, structure, shape, temperature and environment;

— ensure that the application/integration of the authentication elements on the material product and/or its components is adequately performed;

— use quality control principles to verify and record that the application meets the requirements;

— take and record corrective actions in case of failure or insufficient application because the replacement of authentication elements on fraudulent or tampered products should be prevented.

If sealing of the material good or its packaging is required, one or more authentication elements should be present on the seal and/or logically associated with it.

6.6 Data management

Authentication solutions facilitate the detection of material goods that are subject to product fraud.

The organization should record all data related to the selection, sourcing, application and inspection of authentication elements and any issues found (e.g. counterfeiting) for analysis.

Data collection and analysis can be derived from sources such as:

— investigation of suspicious product;

— investigation by mystery shopping;

— investigation by returned good analysis;

— data derived from online verification tools and systems;

— data derived from internet surveillance applications.

NOTE Mystery shopping is defined in ISO 20252:2019, 3.54.

Such data should be stored in a secure database with restricted access for identified users. This data should be used to conduct data analysis and risk analysis.

Security measures to ensure data integrity should be implemented in order to detect data tampering or modifications that could impact authentication.

The value creation chain of the authentication solution should be recorded.

6.7 Effectiveness measurement in normal verification/authentication situations

The organization should, in the normal inspection context, evaluate the following.

— Inspector(s): Identification/authentication, access rights and training.

— Tools: Authentication activity, reduced functionality, maintenance, calibration, downloads and tampering.

— Connections and data exchanges (if required): Successful and denied logins, and quality of service.

— Integrity and security of data associated with the authentication solution, as explained in ISO 22381.

— Results: Sampling rates, number of true/false detections, or number of non-interpretable authentication elements.

NOTE Depending on the type of authentication solution implemented, these indicators can be issued through an automated data collection or through a declaration from the inspectors.

6.8 Effectiveness assessment in emergency verification/authentication situations

In cases of emergency when the counterfeiting detection reaches a defined threshold, the organization should adapt authentication protocols to address the counterfeiting issues.

6.9 Impact of verification results and corrective actions

The organization should assess the overall effectiveness of the solution through the multiple criteria and requirements given in this document. It should apply the PDCA cycle in order to select or adapt the authentication tools and solutions to new risks and threats, as described in 4.2, and should act accordingly.

Annex A
(informative)

Assessment grid

Table A.1 provides a grid for assessing authentication solutions according to the criteria defined in Clause 5.

This grid will help the specifier of the authentication solution to select the relevant performance criteria from the full list of criteria and to select the level of relevance of each criteria.

The relevance should be evaluated for each risk anticipated for the particular material good.

Table A.1 — Assessment criteria

Assessment criteria	Objectives targeted	Parameters to be assessed	Relevance				Assessment
			High	Medium	Low	Not relevant	
1. Physical characteristics of the authentication element	To specify the characteristics of the authentication element in its environment						
1.1 Static characteristics		Size					
		Thickness					
		Weight					
1.2 Dynamic characteristics		Flexibility					
		Viscosity					
		Tear					
		Tensile strength					
1.3 Durability characteristics		Mild environmental conditions					
		Harsh environmental aggression					
		Mechanical use					
		Aging					
1.4 Health and environmental impact characteristics		Electromagnetic radiations					
		Radioactivity					
		Chemical composition					
		Migration of substances					
		Recyclability					

Table A.1 *(continued)*

Assessment criteria	Objectives targeted	Parameters to be assessed	Relevance				Assessment
			High	Medium	Low	Not relevant	
1.5 Feature-linked physical characteristics		Detection by human senses					
		Machine readable					
		Uniqueness					
2. Attack resistance of the authentication elements	To specify the performance of the authentication element regarding different sorts of attacks						
2.1 Resistance to reproduction		Duplication					
		Simulation, emulation					
		Reverse engineering					
2.2 Tamper resistance / Tamper evidence		Tampering resistance					
		Tampering evidence					
2.3 Alteration resistance							
2.4 Side channel resistance							
2.5 Interception of communication							
2.6 Obsolescence							
2.7 Not uncontrolled reuse							
3. Integration process	To specify the performance of the authentication element for integration with the material good						
3.1 Security		Security policy					
		Supply chain security					
3.2 Manufacturing		Availability					
		Compatibility with material good/ packaging					
		Compatibility with process					
		Compatibility with logistics					
		Integrity					
3.3 Compliance							
3.4 Training							

Table A.1 *(continued)*

Assessment criteria	Objectives targeted	Parameters to be assessed	Relevance				Assess-ment
			High	Medi-um	Low	Not rele-vant	
4. Attack resistance of the authentication tools	To specify the performance of the authentication tool regarding different sort of attacks						
4.1 Secret recovery, simulation and emulation		Secret recovery					
		Simulation, emulation					
4.2 Tamper resistance/tamper evidence							
4.3 Alteration resistance							
4.4 Side channel resistance							
4.5 Interception of communication							
4.6 System security							
4.7 Security of database access							
4.8 Redundancy, back up							
4.9 Obsolescence							
4.10 Vulnerability							
5. Criteria for the selection of authentication solutions	To specify the performance of authentication solutions in the field						
5.1 Field environmental function							
5.1.1 Required resources		Power					
		Communication					
		Facilities					
5.1.2 Environmental conditions		Temperature					
		Humidity					
		Dirt					
		Electromagnetic radiation					
		Electrostatic and magnetic fields					
		Air pressure					
5.1.3 Hazardous conditions exposure		Chemical					
		Radioactive					
		Explosive					

Table A.1 *(continued)*

Assessment criteria	Objectives targeted	Parameters to be assessed	Relevance				Assessment
			High	Medium	Low	Not relevant	
5.1.4 Normal usage deterioration		Abrasion					
		Dirt					
5.1.5 Ergonomics		Lighting conditions					
		Rain, humidity, snow					
		Temperature					
		Wind					
5.1.6 Authentication parameters		Authentication cycle time					
		Frequency					
		Concurrent authentication					
		Response time					
5.2 Life cycle							
6. Implementation process	To specify the performance of authentication solution in operation						
6.1 Security policy							
6.2 Compliance		Compliance with regulation					
		Compliance audit					
6.3 Operation		Start time					
		Process, adaptability					
		Upgrade capability					
		Accountability and quality control					
		Multi-use capability					
		Sensibility of results					
		Normal/fallback modes					
		Tool supply environment					
		Training					
		Health environment					
6.4 Efficiency		Usage rate of solution, i.e. quota of items checked versus targeted population of items (sampling according to chosen methodology)					

Table A.1 *(continued)*

Assessment criteria	Objectives targeted	Parameters to be assessed	Relevance				Assess-ment
			High	Medi-um	Low	Not rele-vant	
		False acceptance rate (no alarm on a fake product) and false rejection rate (alarm on genuine product)					
		Data capture and/or retrieval on the authenticity and integrity of the product good					
		Ability of the solution to provide data on the authenticity and integrity of the material good in the market					
7. Data capture	To verify integrity of data captured, recorded and stored	Data capture and/or retrieval on the authenticity and integrity of the product good					
7.1 On authenti-cation element selection		Criteria for selection					
7.2 On sourcing		Supplier					
7.3 On application		Usage					
7.4 From inspection		Inspection activity					
7.5 On issues found		Capture and/or retrieval of product authenticity and integrity data or information					

Annex B
(informative)

Control means access table

Table B.1 provides a tool for rights holders to define their anti-counterfeiting strategy in relation to the inspection of authentication elements. Combinations of technologies can be used to have a high level of protection, but the different layers of authentication elements should not be accessible and controlled by all types of inspector. The rights owners have therefore to define who will have access to what.

Table B.1 — Control means access

Inspector authentication element	End user	Distribution and supplying networks	Supervisory authority	Personnel given clearance by the rights holder	Accredited/ notified laboratory
Overt Verifiable independently by purely human input					
Covert Requires a technical tool					
Forensic analysis Requires testing by a laboratory					

Bibliography

[1] ISO 14298, *Graphic technology — Management of security printing processes*

[2] ISO/IEC 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

[3] ISO 16678, *Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade*

[4] ISO 20252, *Market, opinion and social research, including insights and data analytics — Vocabulary and service requirements*

[5] ISO 22380, *Security and resilience — Authenticity, integrity and trust for products and documents — General principles for product fraud risk and countermeasures*

[6] ISO 22381, *Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for establishing interoperability among object identification systems to deter counterfeiting and illicit trade*

[7] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

[8] ISO 31000, *Risk management — Guidelines*

[9] AFNOR XP Z42-101, *Electronic archiving — Specifications for the implementation of the Visible Digital Seal (VDS) for authentication, verification and acquisition of data carried by an object — General structure*

[10] Ross A. *Relating ROC and CMC Curves*. National Institute of Standards and Technology (NIST), US Department of Commerce, 2016. Available from: https://www.nist.gov/system/files/documents/2016/12/06/12_ross_cmc-roc_ibpc2016.pdf

ICS 03.100.01
Price based on 25 pages